IAC Mission Success Stories

Please visit other DTIC IAC Mission Success Pages by following these links...

AMPTIAC
CBIAC
CPIA
DACS
HSIAC
IATAC
IRIA
MSIAC
MITIAC
NTIAC
RAC
SURVIAC
WSTIAC

Please visit other Military IAC Mission Success Pages by following these links...

AFWIAC
DEIAC
GRSTIAC
GTIAC
DTRIAC
EIAC
HEIAC
SAVIAC
SMIAC

Defense Technical Information Center
ATTN: DTIC-AI
8725 John J. Kingman Road, Suite 0944
Fort Belvoir, VA 22060-6218
Commercial: 703 767 9120
DSN: 427 9120
FAX: 703 767 9119
E-mail: iac@dtic.mil

IATAC

Information Assurance Technology Analysis Center

JTF-CND IAC Success Story

The Joint Task Force for Computer Network Defense (JTF-CND) was activated in December 1998 with a mission to defend the Defense Information Infrastructure (DII) against computer network attacks, and to accomplish this global mission with only 24 personnel. Within months it's mission grew—staff had not. In order to meet its extensive mission requirements, the JTF leveraged IATAC across a broad range of mission support areas, freeing the assigned staff to focus on the critical day-to-day operations. IATAC's relationship with and support to the JTF-CND continues to be a testimony of success!

Continued on Story 1

IATAC Provides Timely Reports

IATAC recently produced a series of reports (both *Critical Review and Technology Assessments* [CR/TA] and a *State-of-the-Art Reports* [SOAR]) for the IA community addressing subjects of critical importance. The topics of these reports are Defense in Depth, Data Mining, IA Metrics, and IO/IA Visualization Technologies. What distinguishes these reports is their timeliness and value to the IA community in providing subject insights, supporting technologies, and ongoing research into these subject areas. Written to educate leaders and managers in the subject at hand, the reports provide critical information to assist them in understanding the complexities of the subject, considerations they should examine, and ultimately assist in key IA decision making—and every report is free to DoD!!!

Continued on Story 2

Please visit our Web site at http://iac.dtic.mil/iatac or send us an E-mail to iatac@dtic.mil

IAC Mission Success Stories

Please visit other DTIC IAC Mission Success Pages by following these links...

AMPTIAC
CBIAC
CPIA
DACS
HSIAC
IATAC
IRIA
MSIAC
MOTIAC
NTIAC
RAC
SURVIAC
WSTIAC

Please visit other Military IAC Mission Success Pages by following these links...

AFMIAC
DEUAC
CRSTIAC
CTIAC
DTRIAC
EIAC
HEIAC
SAVIAC
SMIAC

Defense Technical Information Center
ATTN: DTIC-AI
8725 John J. Kingman Road, Suite 0944
Fort Belvoir, VA 22060-6218
Commercial: 703 767 9120
DSN: 427 9120
FAX: 703 767 9119
E-mail: iac@dtic.mil

IATAC

Information Assurance Technology Analysis Center

IATAC | Story 1 | Story 2

JTF-CND IAC Success Story (continued)

The initial call for support by the JTF was drafting the command's *Tactics, Techniques, and Procedures (TTP)* —in six weeks. IATAC met the challenge. This *TTP* has become a living document, through which the JTF executes its mission with IATAC capturing those operational enhancements in updates. This success has resulted in IATAC becoming an extension of the JTF staff with both onsite support as well as reach back capability in supporting the JTF's growing requirements.

The JTF routinely exercises this reach back support by capturing and drafting JTF positions on a variety of issues confronting the operational, intelligence, law enforcement, and counterintelligence communities. Notable among these have been white papers on Information Operations Conditions (INFOCON), concept development of the JTF-CND based Law Enforcement/CounterIntelligence (LE/CI) Center, responses to Joint Staff instructions, and drafting the JTF's requirements document for the Information Assurance Common Operational Picture (IA COP). The JTF's confidence in IATAC staff has resulted in not only IATAC staff representing the JTF at conferences and symposia, but the planning and executing of all JTF-CND Component Commander's Conferences for the past year.

Leveraging IATAC's strong background in exercise development, the JTF requested IATAC to plan and execute exercise Zenith Star. This exercise examined interagency working-level coordination using a computer network defense scenario similar to Eligible Receiver 97. *Zenith Star* also provided the JTF an opportunity to test and hone its own *TTP*. Exercise support by IATAC continues with ongoing planning and execution of *Tactical Decision Exercises* (TDE) designed to test internal procedures, as well as command wide semi-annual exercises similar in scope to *Zenith Star*.

IATAC has developed a Web based "PlayBook" for the JTF providing a decision support tool which automates the staff actions called for in the *TTP*. A beta-version is currently undergoing testing at the JTF's Joint Operations Center. IATAC has literally become a "force multiplier" for the JTF, allowing it's most precious resource—its staff officers—to tend to the business of defending the DII.

Please visit our Web site at http://iac.dtic.mil/iatac or send us an E-mail to iatac@dtic.mil

Defense Technical Information Center
ATTN: DTIC-AI
8725 John J. Kingman Road, Suite 0944
Fort Belvoir, VA 22060-6218
Commercial: 703 767 9120
DSN: 427 9120
FAX: 703 767 9119
E-mail: iac@dtic.mil

IATAC

Information Assurance Technology Analysis Center

IATAC Provides Timely Reports (continued)

Defense in Depth CR/TA —Attacks on DoD systems have expanded from simple wiretaps and viruses to session hijacks and Trojan horses—and the types and sophistication of these attacks are constantly evolving. In response to these threats, DoD developed the defense in depth strategy to protect its networks and information systems. The execution of the strategy requires a significant number of different security and networking technologies. This report describes the impact of those evolving technologies on the strategy.

Data Mining CR/TA —In its continuing effort to meet the challenge of defending its networks, DoD has employed hundreds of sensors to detect unauthorized activities within those networks and information systems. These sensors produce millions upon millions of alerts and data points daily. Making sense of that data—transforming it into actionable knowledge—is the realm of data mining explored by this CR/TA. It provides an overview of data mining techniques, applications, and COTS data mining software products. It describes the process of determining data mining objectives, preparing data, transforming data, mining data, analyzing data, and assimilating knowledge.

IA Metrics CR/TA —IA metrics provide a way of measuring the effectiveness of the organizationÕs security efforts against a set of specific goals and objectives derived from the organization's mission. In January 2000, the Joint Staff published CJCSI 6510.03, *Information Assurance Readiness Metrics* . This new instruction provided IA metrics for DoD use in preparing the Joint Monthly Readiness Report (JMRR). The IATAC CR/TA draws upon this instruction and provides essential foundational information on IA metrics to help organizations craft their own metrics. It answers the following questions—

- *What are IA metrics?*
- *Why do organizations need them?*
- *How can metrics be used by at each level within an organization?*
- *What is the process for developing IA metrics?*
- *What are some of the IA metrics that are already available and what are their strengths and weaknesses?*
- *What is the future direction for IA metrics?*

IO/IA Visualization Technologies SOAR—Rounding out the suite of reports from IATAC is an examination of one of the great challenges facing the IA community—the ability to display information in a meaningful, actionable manner. This SOAR examines human factors, types, and identification of organizational visualization technologies. It presents current visualization technologies for IA, information operations, battlespace visualization, and common operational picture. The report focuses on technologies that are currently available and applicable to current operations and requirements. It helps leaders to decide whether visualization is appropriate to their needs, to determine what types of visualization technologies are available and relevant, and to formulate possible strategies for implementing visualization solutions.

Please visit our Web site at http://iac.dtic.mil/iatac or send us an E-mail to iatac@dtic.mil